WLAN 시스템에서 무선 채널 기반의 물리계층 인증에 관한 연구

오한올, 윤지현, 김태훈■§, 방인규■*

한밭대학교 정보통신공학과, *지능미디어공학과, §한밭대학교 컴퓨터공학과

{hanol, jyeoning}@edu.hanbat.ac.kr, {thkim, ikbang}@hanbat.ac.kr

A Study on Channel-based Physical-Layer Authentication in WLAN Systems

Hanol Oh, Jihyeon Yoon, Taehoon Kim■§, Inkyu Bang■*

Dept. of Information and Communication Engineering, Hanbat National University

§Dept. of Computer Engineering, Hanbat National University

*Dept. of Intelligence Media Engineering, Hanbat National University

요 약

본 연구에서는 WLAN (Wireless Local Area Network) 네트워크에서 무선 주파수 지문(radio frequency fingerprinting: RFF)과 심층학습(deep learning) 기술을 활용한 물리계층 인증(physical-layer authentication: PLA) 시스템을 구현한다. 제안 시스템은 WLAN 비콘(beacon) 신호의 특성을 CNN 모델을 기반으로 학습하여 합법적 AP (Access Point)와 알려지지 않은 AP, 그리고 위장 공격자를 구분할 수 있다. 추가적으로, 본 연구에서는 위장 공격자의 실제 위치와 훈련 데이터 수집 시에 예상한 위장 공격자 위치 차이에 따른 위장 공격 탐지 성능을 비교 분석한다.

Ⅰ. 서론

WLAN 네트워크는 라우터나 AP를 통해 발생한 무선 신호를 사용하여 다양한 장치들이 네트워크에 연결될 수 있도록 해주는 기술이다. WLAN 표준인 IEEE 802.11에서는 MAC 주소와 SSID와 같은 단순한 디지털 식별자 기반 인증 방법을 사용하는데 이러한 단순한 인증 보안 방법은 라우터 위장 공격을 탐지하는 데에 효과적이지 않다.

라우터 위장 공격(Rogue AP Attack)이란 공격자가 합법적인 AP인 것처럼 위장하여 사용자를 속이는 공격 방식이다. 이러한 공격 방식 중 대표적인 방법으로 공격자가 자신의 MAC 주소를 합법적인 AP의 MAC 주소로 위장하는 MAC Spoofing 공격이 있다. 이러한 형태의 라우터 위장 공격이 발생하면 사용자는 위장된 AP에 연결되어 네트워크 트래픽이 가로채이거나 개인 정보가 탈취될 위험에 처할 수 있다. 따라서 쉽게 변조될 수 없는 RF 신호의 고유한 물리계층 특징을 활용하는 RF Fingerprinting에 관한 연구가 대두되고 있다 [1].

본 논문에서는 WLAN 네트워크에서 무선 채널 기반의 RFF 기법을 활용하여 다양한 상황에서 라우터 위장 공격자를 탐지하는 실험을 수행하고 위장 공격 탐지 성능을 비교한다.

Ⅱ. 시스템 모델 및 분석 방법

본 연구에서는 그림 1과 같이 WLAN 네트워크에서 송수신기 간 무선 채널을 이용한 RFF 기법과 CNN 분류 모델을 활용하여 라우터 위장 공격자를 식별하기 위한 물리계층 인증 시스템을 고려한다. 공격자가 자신의 MAC 주소를 합법적 AP의 MAC 주소로 위장하여 사용자에게 비콘 프레임을 송신할 때, 공격자의 RFF가 합법적 AP의 RFF와 다르다는 점을 활용하여 위장 공격자를 탐지할 수 있다.

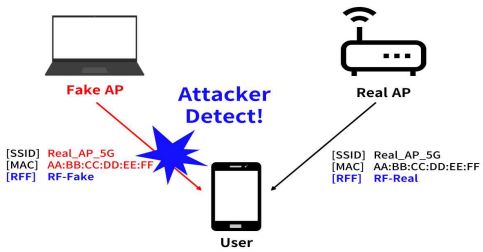


그림 1. 시스템 모델

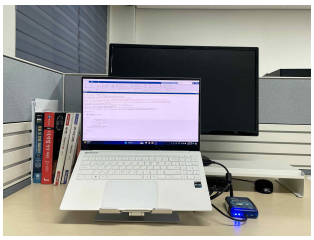
본 논문에서는 공격자가 특정 위치에 있을 것이라 가정하고 훈련 데이터를 수집하여 공격자 분류 모델을 생성하는 상황을 다룬다. 합법적 AP 클래스(Known AP)와 알려지지 않은 AP 클래스(Unknown AP)에 대한 비콘 데이터를 수집하고, 임의로 가정한 공격자 위치에서 Attacker 클래스 비콘 데이터를 수집하였다. 수집한 3000개의 비콘에서 L-LTF 필드와 MAC 주소를 추출하여 각각 훈련 데이터와 라벨 값으로 사용하였다. 훈련 데이터를 'Known', 'Unknown', 'Attacker' 범주로 라벨링하여 CNN 모델로 지도학습을 진행하였다. 은닉층에 2개의 합성곱층과 최대 풀링층, 3개의 완전 연결층을 두었고 배치 정규화와 ReLU 층을 활용하였으며 출력층에는 softmax 활성화 층을, 옵티마이저로는 Adam을 사용하여 CNN 모델을 구현하였다 [2]. 훈련 결과로 생성된 모델에 실제 위장 공격자의 위치에서 생성된 테스트 데이터를 입력하여 위장 공격 탐지 성능을 비교한다.

Ⅲ. 실험 환경 및 결과

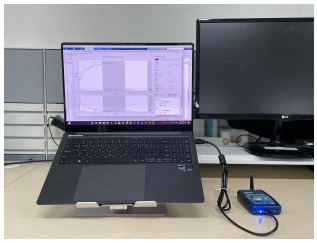
1) 실험 환경

실험을 위해 합법적 AP와 위장 공격자를 구현할 비콘 송신용 SDR 1개(그림 2-(a))와 비콘 데이터를 수집하여 공격자 탐지 모델을 생성할 수신용 SDR 1개(그림 2-(b)), 총 2개의 SDR을 사용한다. 본 연구의 실험 진행을 위해 'ADALM-PLUTO' SDR 기기를 사용하였다.

■ Corresponding Authors: Taehoon Kim and Inkyu Bang



(a) 비콘 송신용 SDR에 연결된 노트북

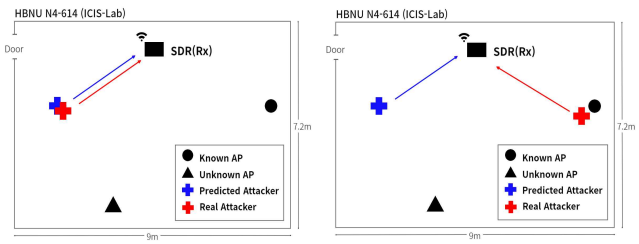


(b) 비콘 수신용 SDR에 연결된 노트북

그림 2. 실험 환경

2) 실험 시나리오

본 연구에서는 그림 3과 같이 새로운 테스트 데이터 수집 환경에 따라 2가지 실험을 진행하였다. 실험 (1)에서는 가정한 공격자 위치와 가까운 위치에서 새로운 위장 비콘 테스트 데이터를 생성하여 훈련된 모델에 입력하였다. 즉 실제 공격자가 가정한 공격자 위치와 비슷한 위치에 있는 상황을 고려하였다. 실험 (2)에서는 합법적 AP와 가까운 위치에서 위장 비콘 테스트 데이터를 생성하여 훈련된 모델에 입력하였다. 즉, 실제 공격자가 모델 생성 단계에서 가정한 위치가 아니라 위장 대상인 합법적 AP와 비슷한 위치에 있는 상황을 고려하였다.



실험 (1) 실제 공격자 위치가 예상한 공격자 위치와 비슷한 상황

실험 (2) 실제 공격자 위치가 위장 대상 위치와 비슷한 상황

그림 3. 실험 시나리오

3) 실험 결과

표 1은 수집한 훈련용 데이터의 일부를 테스트 데이터로 만들어 훈련된 모델의 분류 정확도를 나타내는 결과표이다.

표 1. Confusion matrix (detection accuracy = 97.13%)

	Known	Unknown	Attacker
Known	94.7%	3%	2%
Unknown	0%	100%	0%
Attacker	0.3%	3%	**96.7%**

표 2는 실험 (1)의 분류 정확도를, 표 3은 실험 (2)의 분류 정확도를 나타내는 결과표이다.

표 2. Confusion matrix (detection accuracy = 95.9%)

	Known	Unknown	Attacker
Known	94.7%	3%	2%
Unknown	0%	100%	0%
Attacker	4%	3%	**93%**

표 3. Confusion matrix (detection accuracy = 82.8%)

	Known	Unknown	Attacker
Known	94.7%	3%	2%
Unknown	0%	100%	0%
Attacker	41.6%	4.7%	**53.7%**

실제 공격자가 예상한 공격자 위치와 비슷한 위치에서 공격하는 상황에서는 93%의 높은 위장 공격자 탐지 정확도를 보인다.(표 2) 하지만 실제 공격자가 위장 대상인 Known과 비슷한 위치에 있을 때에는 53.7%로 낮은 위장 공격자 탐지 정확도를 보인다.(표 3) 이를 통해 가정한 위장 공격자의 위치에서 실제 공격이 발생했을 때에는 높은 정확도로 라우터 위장 공격자를 탐지할 수 있으나, 실제 공격자가 합법적 AP와 비슷한 위치에서 공격을 수행했을 땐 공격자를 탐지하는 성능이 감소함을 확인할 수 있다.

Ⅳ. 결론

본 논문에서는 WLAN 네트워크에서 무선 채널 기반의 RFF 기법과 CNN 신경망을 활용하여 다양한 상황에서의 라우터 위장 공격자 탐지 성능을 비교하였다. 실험 결과를 통해 훈련 데이터 수집 시에 가정한 공격자 위치와 비슷한 위치에서 실제로 공격이 발생했을 때에는 채널 기반 RFF 인증 보안 기법을 활용하여 위장 공격자를 높은 정확도로 탐지할 수 있으나, 실제 공격자가 위장 대상인 AP와 비슷한 위치에 존재한다면 해당 기법을 사용하는 데에는 어려움이 있음을 확인할 수 있었다.

이러한 한계를 극복하기 위해 송신기 하드웨어의 고유한 특성을 활용한 RFF 기법에 대한 추가적인 연구가 필요하며 본 연구의 후속 연구로 이를 고려하고 있다. 더 나아가, 드론 네트워크와 같은 이동성 있는 환경에서도 활용 가능한 RFF 기법에 대한 연구도 본 연구의 후속 연구로 고려해보고자 한다. 이러한 연구는 WLAN 네트워크의 보안 강화를 위한 중요한 발전 가능성을 제시할 것으로 기대된다.

ACKNOWLEDGMENT

본 논문은 한밭대학교 공학교육혁신센터 “창의 융합형 공학 인재 양성 지원 사업”의 지원과 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2022R1F1A1076126).

참 고 문 헌

[1] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis and K. Chowdhury, "ORACLE: Optimized Radio clAssification through Convolutional neuraL nEtworks," IEEE INFOCOM 2019 - IEEE Conference on Computer Communications, Paris, France, 2019, pp. 370-378.

[2] MATLAB. Version 2023b, “Test a Deep Neural Network with Captured Data to Detect WLAN Router Impersonation” link: https://kr.mathworks.com/help/comm/ug/test-a-deep-neural-network-with-captured-data-to-detect-wlan-router-impersonation.html